CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this correspondence (along with any paper referred to as being attached or enclosed) is being faxed to **571-273-8300** on the date shown below to **Mail Stop Appeal Brief - Patents**, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Date: January 3, 2011 /Robin Wardzala/
Robin Wardzala

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:

Appellant(s):	David D. Brandt, *et al.*	Examiner:	Ronald Baum
Serial No:	10/661,696	Art Unit:	2439
Filing Date:	September 12, 2003		

Title: SYSTEM AND METHODOLOGY PROVIDING AUTOMATION SECURITY ANALYSIS, VALIDATION, AND LEARNING IN AN INDUSTRIAL CONTROLLER ENVIRONMENT

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Dear Sir:

Appellant submits this brief in connection with an appeal of the above-identified patent application. A credit card payment form is filed concurrently herewith in connection with all fees due regarding this appeal brief. In the event any additional fees may be due and/or are not covered by the credit card, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1063 [ALBRP303USC].

TABLE OF CONTENTS

I. Real Party in Interest (37 C.F.R. §41.37(c)(1)(i))…………………………..Page 3

II. Related Appeals and Interferences (37 C.F.R. §41.37(c)(1)(ii))………………Page 4

III. Status of Claims (37 C.F.R. §41.37(c)(1)(iii))……………………………….. Page 5

IV. Status of Amendments (37 C.F.R. §41.37(c)(1)(iv))………………………….Page 6

V. Summary of Claimed Subject Matter (37 C.F.R. §41.37(c)(1)(v))……………Page 7

VI. Grounds of Rejection to be Reviewed (37 C.F.R. §41.37(c)(1)(vi))…………Page 11

VII. Argument (37 C.F.R. §41.37(c)(1)(vii))………………………………………Page 12

Conclusion………………..……………………………………………………Page 21

VIII. Claims Appendix……..………………………………………………………Page 22

IX. Evidence Appendix…………………………………………….……………...Page 33

X. Related Proceedings Appendix (37 C.F.R. §41.37(c)(1)(x))...………………...Page 34

I. Real Party in Interest (37 C.F.R. §41.37(c)(1)(i))

The real party in interest in the present appeal is Rockwell Automation Technologies, Incorporated, the assignee of the present application.

II. Related Appeals and Interferences (37 C.F.R. §41.37(c)(1)(ii))

Appellant is not aware of any appeals or interferences which may be related to, will directly affect, or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims (37 C.F.R. §41.37(c)(1)(iii))

Claims 1-9, 12-17, 19-21, 23, 25, 30, 41, and 45-52 stand rejected and are under appeal.

IV. Status of Amendments (37 C.F.R. §41.37(c)(1)(iv))

Amendments filed concurrently with the RCE, filed on May 21, 2010, were entered and examined by the Examiner, as indicated in the subsequent Office Action, dated August 2, 2010.

V. Summary of Claimed Subject Matter (37 C.F.R. §41.37(c)(1)(v))

A. Independent Claim 1

Independent claim 1 is directed toward a security analysis tool for an automation system having a controller, an I/O device, and a controlled device (see *e.g.*, paragraph [0031]), the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store the input data and the output data in an I/O table (see, *e.g.*, paragraph [0004]), the memory further configured to store a control program that uses the I/O table to control the controlled device, the security analysis tool comprising a learning component that monitors the communication of data associated with the I/O table during a training period and generates a learned pattern of communication (see, *e.g.*, paragraph [0013], [0050], [0053]-[0057], and [0073] and Figures 7, 9, and 12), and an analyzer component that monitors data traffic subsequent to the training period (see, *e.g.*, paragraphs [0014], [0064], and [0074] and Figures 9 and 12) and generates one or more security outputs if a current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation (see, *e.g.*, paragraphs [0014] and [0075] and Figure 12), the one or more security outputs including at least one output that alters the data traffic between the controller and the at least on I/O device (see, *e.g.*, paragraph [0075]).

B. Independent Claim 12

Independent claim 12 is directed toward a method for us in an industrial automation system having an industrial controller, an I/O device, and a controlled device (see *e.g.*, paragraph [0031]), the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the industrial controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the industrial controller also having a memory configured to store the input data and output data in an I/O table (see, *e.g.*, paragraph [0004]), the memory further configured to store a control program that uses the I/O table to control the controlled device, the method comprising monitoring communication of data associated with the I/O table for a predetermined training period to learn at least one learned access pattern of communication (see, *e.g.*, paragraph [0013], [0050], [0053]-[0057], and [0073] and Figures 7, 9, and 12), defining a pattern threshold specifying an acceptable deviation from the at least one learned pattern (see, *e.g.*, paragraph [0059]), monitoring data traffic subsequent to the training period (see, *e.g.*, paragraphs [0014], [0064], and [0074] and Figures 9 and 12), and performing at least one automated security event if a current pattern of the data traffic deviates from the at least one learned pattern in excess of the acceptable deviation after the training period (see, *e.g.*, paragraphs [0014] and [0075] and Figure 12), wherein the performing the at least one automated security event includes at least altering a network traffic pattern between the industrial controller and the I/O device (see, *e.g.*, paragraph [0075]).

C. <u>Independent Claim 16</u>

Independent claim 16 is directed toward a security analysis system in an industrial automation environment having an industrial controller, an I/O device, and a controlled device (see *e.g.*, paragraph [0031]), the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the industrial controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the industrial controller also having a memory configured to store the input data and output data in an I/O table (see, *e.g.*, paragraph [0004]), the memory further configured to store a control program that uses the I/O table to control the controlled device, the security analysis system comprising means for monitoring communication of data associated with the I/O table for a predetermined period, means for learning at least one learned pattern of communication based on the means for monitoring (see, *e.g.*, paragraph [0013], [0050], [0053]-[0057], and [0073] and Figures 7, 9, and 12), means for defining a pattern threshold that specifies an acceptable deviation from the learned pattern (see, *e.g.*, paragraph [0059]), means for automatically detecting that a current pattern of communication of the data associated with the I/O table deviates from the learned pattern in excess of the acceptable deviation after the training period (see, *e.g.*, paragraphs [0014], [0064], [0074] and [0075] and Figures 9 and 12), and means for performing an automated action that alters the current pattern of communication in response to the detecting (see, *e.g.*, paragraph [0075]).

D. Independent Claim 17

Independent claim 17 is directed toward a security validation system for use in an industrial automation environment having an industrial controller, an I/O device, and a controlled device (see *e.g.*, paragraph [0031]), the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the industrial controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the industrial controller also having a memory configured to store the input data and output data in an I/O table (see, *e.g.*, paragraph [0004]), the memory further configured to store a control program that uses the I/O table to control the controlled device, the system comprising a learning component that monitors communication of data associated with the I/O table with respect to the industrial controller during a training period and establishes a learned pattern of communication (see, *e.g.*, paragraph [0013], [0050], [0053]-[0057], and [0073] and Figures 7, 9, and 12), and an analyzer component that monitors a current pattern of communication of the data associated with the I/O table subsequent to the training period (see, *e.g.*, paragraphs [0014], [0064], and [0074] and Figures 9 and 12) and automatically performs a security action to bring the current pattern in line with the learned pattern in response to detecting that the current pattern communication has deviated from the learned pattern of access in excess of a defined pattern threshold (see, *e.g.*, paragraphs [0014] and [0075] and Figure 12).

E. Independent Claim 30

Independent claim 30 is directed toward an automated security validation system for use in an industrial automation environment having an industrial controller, an I/O device, and a controlled device (see *e.g.*, paragraph [0031]), the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the industrial controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the industrial controller also having a memory configured to store the input data and output data in an I/O table (see, *e.g.*, paragraph [0004]), the memory further configured to store a control program that uses the I/O table to control the controlled device, the automated security validation system comprising means for monitoring communication of data associated with the I/O table with respect to the industrial controller during a training period and establishing a learned pattern of communication (see, *e.g.*, paragraph [0013], [0050], [0053]-[0057], and [0073] and Figures 7, 9, and 12), means for defining a pattern threshold specifying an allowable deviation from the learned pattern (see, *e.g.*, paragraph [0059]), means for monitoring a current pattern of communication of the data associated with the I/O table subsequent to the training period (see, *e.g.*, paragraphs [0014], [0064], and [0074] and Figures 9 and 12), and means for initiating a security procedure that performs a security action to bring the current pattern in line with the learned pattern if the means for monitoring identifies that a current access pattern deviates from the at least learned pattern in excess of the allowable deviation (see, *e.g.*, paragraphs [0014] and [0075] and Figure 12).

VI. Grounds of Rejection to be Reviewed (37 C.F.R. §41.37(c)(1)(vi))

A. Whether claims 1-9, 12-17, 19-21, 23, 25, 30, 41, and 45-52 are patentable under 35 U.S.C. §103(a) over Swiler, *et al.* (U.S. Patent 7,013,395 B1) in view of Townsend (U.S. Patent 6,374,358 B1), and further in view of Godwin (U.S. Patent Publication No. 2004/0059920 A1).

VII. Argument (37 C.F.R. §41.37(c)(1)(vii))

A. Rejection of Claims 1-9, 12-17, 19-21, 23, 25, 30, 41, and 45-52 Under 35 U.S.C. §103(a)

Claims 1-9, 12-17, 19-21, 23, 25, 30, 41, and 45-52 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Swiler, *et al.*, (U.S. 7,013,395 B1) in view of Townsend (U.S. 6,374,358 B1), and further in view of Godwin (U.S. 2004/0059920 A1). It is believed that this rejection should be reversed for at least the following reasons. Swiler, *et al.*, Townsend, and Godwin, individually or in combination, do not disclose or suggest all features set forth the subject claims.

> To reject claims in an application under § 103, an examiner must establish a prima facie case of obviousness. A prima facie case of obviousness is established by a showing of three basic criteria. First, there must be some apparent reason to combine the known elements in the fashion claimed by the patent at issue (*e.g.*, in the references themselves, interrelated teachings of multiple patents, the effects of demands known to the design community or present in the marketplace, or in the knowledge generally available to one of ordinary skill in the art). To facilitate review, this analysis should be made explicit. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. See MPEP § 706.02(j). See also KSR Int'l Co. v. Teleflex, Inc., 550 U.S. 398, 04-1350, slip op. at 14 (2007). The reasonable expectation of success must be found in the prior art and not based on applicant's disclosure. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)

1. Swiler, *et al.*, Townsend, and Godwin fail to disclose or reasonably suggest "a learning component that monitors the communication of data associated with the I/O table during a training period and generates a learned pattern of communication" - Claims 1-9, 12-17, 19-21, 23, 25, 30, 41, 45-52

The present application relates generally to network and automation device security in an industrial automation environment. According to one or more embodiments, a network-based security learning system (*e.g.*, a learning component) can be provided that monitors an automation network during a predetermined training period. During the training period, the learning component can monitor and learn activities or patterns such as the number of network requests to and from one or more assets, the type of requests, status or counter data, or substantially any data type or pattern that can be retrieved from the network or asset. After the training period, the learning component can monitor the automation network or assets for detected deviations from data patterns learned during the training period. If desired, a user interface can be provided, wherein one or more pattern thresholds can be adjusted. An alarm or automated event can then occur if a deviation is detected outside the threshold (see, *e.g.*, page 5, line 11 - page 6, line 5). In particular, independent claim 1 recites, *a learning component that* ***monitors the communication of data associated with the I/O table during a training period and generates a learned pattern of communication****.*

Swiler, *et al.* does not disclose or suggest at least these features. Swiler, *et al.* relates to an analysis tool that assesses potential security risks in a network. This analysis tool uses as input a database of common attacks broken into atomic steps, specific network configuration and topology information, and an attacker profile. The attack information is matched with the network configuration information and an attacker profile to create an attack graph. Graph algorithms are then applied to the attack graph to identify attack paths with the highest probability of success (see column 3, line 67 - column 4, line 11).

However, the analysis tool described in Swiler, *et al.* does not *monitor communication of data associated with an I/O table during a training period*, or *generate a learned pattern of communication*. Rather, column 4, lines 43-58 of Swiler, *et al.* describe the three types of input employed by the analysis tool to generate an attack graph as being *attack templates*, a *configuration file*, and an *attacker profile*. The attack templates and attacker profile represent generic information about hypothetical attacker capabilities and attack steps. Since this information represents generic information that is not actively monitored, the attack templates and attacker profile inputs do not read on nor suggest *monitoring communication of data during a training period and generating a learned pattern of communication*. The other type of input into the cited analysis tool, the configuration file, is described in Swiler, *et al.* as follows:

> "The configuration file contains *initial architectural information* about the specific system to be analyzed including the *topology of the networks* and detailed *configurations of particular network elements such as workstations, servers, or routers*. The configuration files include categorical labels all known exploitable configurations (*e.g.* blank administrator password) and are used as triggers for state changes." (column 4, lines 47-54) (Emphasis added).

As can be seen, the configuration file does not represent monitored communication of data, but rather encodes *architectural information* regarding the system being analyzed (*e.g.*, network topologies, device configurations, *etc.*). Swiler, *et al.* nowhere states that the analysis tool described therein has the capability to *monitor communication of data* in general, and therefore fails more specifically to disclose or reasonably suggest *monitoring the communication of data associated with the I/O table during a training period and generating a learned pattern of communication*.

In the Office Action dated August 2, 2010, the Examiner contends that Swiler, *et al.* discloses these aspects, stating on page 4:

> "…whereas the provided computer system analysis tool using *inputted computer system/network configuration/topology (i.e. description of factory assets inclusive of system information acquisition ('...a learning component...monitors the communication of data...during a training period') as part of the monitoring/scanning of communication to/from the network computer*, whereas for the case of factory automation IT/network elements involved in the operation of a given commercial/industrial/government environment…encompass the use of – at the very least – programmable logic controllers of which industrial controllers are an associated architecture), such that industrial controllers running standard operating systems…use I/O data structures to at least deal with interface processing (*e.g.*, I/O tables involved in port communications (i.e., hardware driver support of serial ports, parallel ports, USB ports, and communications ports that deal with both a port physical network address and associated application involved during packet communications generally; 'I/O device…I/O table…') processing, *etc.*), *clearly dealing with Intranet/Internet access patterns insofar as network security per se is concerned*) and *attack template (i.e., a model; 'generates a learned pattern of communication...')* information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner."

At lines 1-5 of the above passage, the Examiner ostensibly argues that network configuration/topology information provided to the cited analysis tool *via* the configuration file described above reads on the act of monitoring communication of data during a training period, and goes so far as to assert that the cited analysis tool uses this topology information "as part of the monitoring/scanning of communication to/from the network computer." However, this assertion is not borne out in Swiler, *et al.*, which nowhere indicates that the analysis tool is employed to perform "monitoring/scanning of communication to/from [a] network computer." Rather, as noted *supra*, Swiler, *et al.* receives only *attack templates*, *configuration files*, and *attacker profiles* as inputs, and does not *monitor communication of data* within the system being analyzed, much less *generates a learned pattern of communication*. Moreover, Swiler, *et al.* merely uses this input information to generate an attack graph, which itself performs no active monitoring but instead only identifies a set of *potential* attack paths that have a high probability of success for a hypothetical attacker (see, *e.g.*, column 1, lines 20-23; column 3, lines 16-19; column 4, lines 4-11).

Townsend is also silent regarding these aspects. Townsend relates to a method for selecting a security model for protecting an application from attack by unauthorized sources. To this end, a current countermeasure strength level and a recommended countermeasure strength level are determined for each of at least one countermeasure based on input data and security risk data. A security model including at least one countermeasure and a corresponding strength level is determined based on the current and the recommended strength levels (see column 2, lines 19-29). However, like Swiler, *et al.*, Townsend's countermeasure selection system does not *monitor communication of data and generate a learned pattern of communication*. In this regard, column 3, lines 34-50 describe the information provided to Townsend's system as follows:

> "Consistent with the present invention, information is gathered that *describes the application assets and system architecture of the organization, details about daily operations, and the countermeasures employed at the time of the assessment* (state 110). In one implementation, th*is information is obtained by using a questionnaire that is answered by personnel familiar with the organization's operations*, although other mechanisms for obtaining the information may be used such as, for example, automated interrogation of computer configurations and

> networked security services. The questionnaire is tailored to solicit information consistent with the parameters identified above. For example, if corporate training is identified as a countermeasure, then the questionnaire will ask questions such as how often training is performed, what type of training is given, and who delivers the training. One example of a questionnaire consistent with the present invention is shown in FIG. 2." (Emphasis added)

As made evident by this passage, the inputs employed by Townsend's countermeasure selection tool comprise information about the network being assessed that can be *provided via a questionnaire*. This clearly does not include monitored communication of data. Since Townsend does not monitor communication of data within the network, the cited reference also fails to disclose or suggest *generating a learned pattern of communication.*

Godwin does not cure the above deficiencies. Godwin relates to a tool for checking storage management system security settings. This tool accesses one or more security parameters, compares them to security policies, rules, and allowable values, and reports noncompliant settings *via* a user-readable report. According to Godwin, a set of automatic correction rules may also be employed to automatically modify noncompliant settings to bring them into compliance (see Abstract). However, these parameter checks do not involve any manner of assessment on network access patterns generally. Rather, Godwin merely performs a check on each storage security parameter to ensure the parameter is within a compliant range. As such, Godwin fails to remedy the shortcomings of the other cited references with regard to *monitoring the communication of data associated with the I/O table during a training period and generating a learned pattern of communication.*

2. Swiler, *et al.*, Townsend, and Godwin fail to disclose or reasonably suggest "an analyzer component that monitors data traffic subsequent to the training period and generates one or more security outputs if a current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation" - Claims 1-9, 12-17, 19-21, 23, 25, 30, 41, 45-52

Independent claim 1 goes on to recite, *an analyzer component that* ***monitors data traffic subsequent to the training period*** *and* ***generates one or more security outputs if a current pattern of the data traffic deviates from the learned pattern in excess of the acceptable***

***deviation**, the one or more security outputs including at least one output that alters the data traffic between the controller and the at least one I/O device.* As noted above, none of Swiler, *et al.*, Townsend, or Godwin disclose or suggest *monitoring the communication of data associated with the I/O table during a training period and generating a learned pattern of communication.* Since none of those cited references generate or otherwise employ a learned pattern of communication, it follows that the cited references are also silent with regard to generating one or more security outputs if a current pattern of data traffic deviates from such a learned pattern in excess of an acceptable deviation. The Examiner again contends that Swiler, *et al.* discloses these aspects, stating on page 5 of the Office Action:

> "...the provided computer system analysis tool using *inputted computer system/network configuration/topology and attack template information*, such that results (i.e., post analysis generated security outputs; '...generates one or more security outputs...') used to evaluate *(i.e.* graphed output information)*/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (relative to the learned/acquired model/template; '...from the learned pattern...'),* clearly encompassing the claimed limitations as broadly interpreted by the examiner." (Emphasis added)

Here, the Examiner appears to argue that by recommended configuration changes "as a function of the risks and costs associated with the changes recommended," Swiler, *et al.* renders obvious the technique of *monitoring data traffic* subsequent to the training period described above and *generating one or more security outputs if a current pattern of the data traffic deviates from the learned pattern in excess of an acceptable deviation.* However, as noted above, Swiler, *et al.* does not *monitor communication of data associated with an I/O table* in any context, either concurrently with or subsequent to a training period during which a learned pattern of communication is generated. Consequently, Swiler, *et al.* makes no determination regarding whether a *current pattern of data traffic deviates from a learned pattern* in excess of an acceptable deviation. At lines 6-7 of the above-quoted passage of the Office Action, the Examiner ostensibly equates the attack graph of Swiler, *et al.* ("learned/acquired model/template") with the learned pattern of communication recited in independent claim 1. However, since this attack graph merely identifies a set of potential *network attack paths* that can be leveraged by a hypothetical attacker, and does not represent a *learned pattern of communication* gleaned by monitoring communication of data on a network, it is unclear what measure is being identified by the Examiner as "deviating" from this attack graph. Given that the attack graph relied upon in the Office Action has no apparent corresponding measure with which it can be compared to determine a "deviation," the Examiner appears to be performing a hindsight analysis of Swiler, *et al.* using Appellants' claims as reference. It is therefore submitted that Swiler, *et al.* fails to disclose or suggest an analyzer component that *monitors data traffic subsequent to the training period and generates one or more security outputs if a current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation.* Townsend and Godwin do not make up these shortcomings, since, like Swiler, *et al.* those references are also silent with regard to monitoring data traffic generally, and as such fail to render obvious *generating one or more security outputs if a current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation.*

Given the failure of Swiler, *et al.*, Townsend, and Godwin to disclose at least the aspects discussed in arguments 1 and 2 above, it is submitted that the combination of these reference fails to render obvious all aspects recited in independent claim 1, as well as independent claims 12, 16, 17, 19, and 30, which recite similar aspects. It is therefore respectfully requested that the rejection of claims 1, 12, 16, 17, 19, and 30 (and all claims depending there from) be reversed.

3. Swiler, *et al.*, Townsend, and Godwin fail to disclose or reasonably suggest "the analyzer component further performs an automated action that disables network requests from at least one outside network upon detecting that the current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation" - Claim 49

As noted above, one or more embodiments of the present application can generate an alarm or automated event if a deviation from the learned pattern of communication is detected outside the threshold. This automated event can include, for example, automatically disabling all network requests from other networks if the current pattern of data traffic deviates from the learned pattern in excess of the deviation (see, *e.g.*, paragraph [0059]). In particular, claim 49 recites, *the analyzer component further performs an automated action that disables network* *requests from at least one outside network upon detecting that the current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation.*

As discussed *supra*, Swiler, *et al.* is silent with regard to *generating one or more security outputs if a current pattern of the data traffic deviates from the learned pattern in excess of an acceptable deviation.* The cited reference also fails to disclose that these one or more security outputs can include an automated action that disables network requests from at least one outside network. Indeed, Swiler, *et al.* does not generate any manner of security output that alters operation of a network, contrary to the Examiner's assertions on page 29 of the Office Action that the recommendations produced by Swiler, *et al.*'s security analysis tool are used to "make configuration changes in the network to counter vulnerabilities." Rather, the only output produced by the analysis tool described in Swiler, *et al.* is the above-mentioned attack graph, which is only employed for informational purposes in order to assess a risk to network assets. Swiler, *et al.* nowhere indicates that the analysis tool, or the attack graph generated thereby, are capable of implementing countermeasures on the network, and consequently fails to disclose or suggest *performing an automated action that disables network requests from at least one outside network* upon detecting that the current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation.

Townsend shares this deficiency, since the countermeasure selection tool described in that cited reference also fails to generate such security outputs. With regard to outputs, Townsend merely generates a written report of one or more countermeasures and corresponding strength levels, the report including a recommendation for countermeasure implementation (see, *e.g.*, column 8, lines 1-13). However, Townsend does not control or alter operation of a network in any way, and therefore fails in particular to contemplate *performing an automated action that disables network requests from at least one outside network.*

Godwin does not cure the above deficiencies. Examiner appears to argue on page 29 of the Office Action that combining Godwin's security health checking tool with the other cited references renders obvious the act of performing an automated action that disables network requests from at least one outside network, noting in particular that Godwin's tool can change security settings if the settings do not comply with a specification as determined by a compliance check (see, *e.g.*, paragraphs [0071]-[0078] of Godwin). However, Godwin does not indicate that the security parameters subject to this compliance check include parameters that control whether network requests from an outside network are enabled or disabled. Consequently, Godwin discloses no mechanisms or criteria for disabling network requests from at least one outside network, and in particular fails to contemplate performing such an action in response to detecting that a current pattern of the data traffic deviates from a learned pattern in excess of an acceptable deviation.

In view of at least the foregoing, reversal of the rejection of claim 49 is respectfully requested.

B. Conclusion

For at least the above reasons, the claims currently under consideration are believed to be patentable over the cited references. Accordingly, it is respectfully requested that the rejections of claims 1-9, 12-17, 19-21, 23, 25, 30, 41, and 45-52 be reversed.

If any additional fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP303USC].

Respectfully submitted,

Dated: January 3, 2011

By: /Brian Steed/
Brian Steed, Reg. No. 64,095

TUROCY & WATSON, LLP
127 Public Square
57th Floor, Key Tower
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731

VIII. Claims Appendix (37 C.F.R. §41.37(c)(1)(viii))

1. A security analysis tool for an automation system having a controller, an I/O device, and a controlled device, the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store a control program that uses the I/O table to control the controlled device, the security analysis tool comprising:

a learning component that monitors the communication of data associated with the I/O table during a training period and generates a learned pattern of communication; and

an analyzer component that monitors data traffic subsequent to the training period and generates one or more security outputs if a current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation, the one or more security outputs including at least one output that alters the data traffic between the controller and the at least one I/O device.

2. The tool of claim 1, further comprising an interface component that generates a description of one or more industrial controllers in the automation system.

3. The tool of claim 2, wherein at least one of the interface component or the analyzer component operate on a computer and receive one or more factory inputs that provide the description, the factory inputs include at least one of user input, model inputs, schemas, formulas, equations, files, maps, or codes.

4. The tool of claim 3, wherein the factory inputs are processed by the analyzer component to generate the security outputs, the security outputs including at least one of manuals, documents, schemas, executables, codes, files, e-mails, recommendations, topologies, configurations, application procedures, parameters, policies, rules, user procedures, or user practices that are employed to facilitate security measures in an automation system.

5. The tool of claim 2, wherein the interface component includes at least one of a display output having associated display objects and at least one input to facilitate operations with the analyzer component, the interface component is associated with at least one of an engine, an application, an editor tool, a web browser, or a web service.

6. The tool of claim 5, wherein the display objects include at least one of configurable icons, buttons, sliders, input boxes, selection options, menus, or tabs, the display objects having multiple configurable dimensions, shapes, colors, text, data and sounds to facilitate operations with the analyzer component.

7. The tool of claim 5, the at least one input includes user commands from at least one of a mouse, a keyboard, speech input, a web site, a remote web service, a camera, or video input to affect operations of the interface component and the analyzer component.

8. The tool of claim 2, wherein the description includes a model of one or more industrial automation assets to be protected and associated network pathways to access the one or more industrial automation assets.

9. The tool of claim 2, wherein the description includes at least one of risk data or cost data that is employed by the analyzer component to determine suitable security measures.

10-11. (Cancelled)

12. A security analysis method for use in an industrial automation system having an industrial controller, an I/O device, and a controlled device, the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the industrial controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the industrial controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store a control program that uses the I/O table to control the controlled device, the method comprising:

monitoring communication of data associated with the I/O table for a predetermined training period to learn at least one learned pattern of communication;

defining a pattern threshold specifying an acceptable deviation from the at least one learned pattern;

monitoring data traffic subsequent to the training period; and

performing at least one automated security event if a current pattern of the data traffic deviates from the at least one learned pattern in excess of the acceptable deviation after the training period,

wherein performing the at least one automated security event includes at least altering a network traffic pattern between the industrial controller and the I/O device.

13. The method of claim 12, further comprising:

inputting at least one model related to one or more industrial controllers;

generating one or more security outputs based on the at least one model; and automatically installing one or more security components based at least in part on the one or more security outputs.

14. The method of claim 13, wherein generating the one or more security outputs includes generating one or more security outputs that include at least one of recommended security components, codes, parameters, settings, related interconnection topologies, connection configurations, application procedures, security policies, rules, user procedures, or user practices.

15. The method of claim 13, further comprising:

automatically deploying the one or more security outputs to the industrial controller; and

utilizing the one or more security outputs to mitigate at least one of unauthorized network access or network attack.

16. A security analysis system in an industrial automation environment having an industrial controller, an I/O device, and a controlled device, the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the industrial controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the industrial controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store a control program that uses the I/O table to control the controlled device, comprising:

means for monitoring communication of data associated with the I/O table for a predetermined training period;

means for learning at least one learned pattern of communication based on the means for monitoring;

means for defining a pattern threshold that specifies an acceptable deviation from the learned pattern;

means for automatically detecting that a current pattern of communication of the data associated with the I/O table deviates from the learned pattern in excess of the acceptable deviation after the training period; and

means for performing an automated action that alters the current pattern of communication in response to the detecting.

17. A security validation system for use in an industrial automation environment having an industrial controller, an I/O device, and a controlled device, the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the industrial controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the industrial controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store a control program that uses the I/O table to control the controlled device, the system comprising:

a learning component that monitors communication of data associated with the I/O table with respect to the industrial controller during a training period and establishes a learned pattern of communication; and

an analyzer component that monitors a current pattern of communication of the data associated with the I/O table subsequent to the training period and automatically performs a security action to bring the current pattern in line with the learned pattern in response to detecting that the current pattern communication has deviated from the learned pattern of access in excess of a defined pattern threshold.

18. (Cancelled)

19. The system of claim 17, further comprising:

a scanner component that automatically interrogates at least one of the industrial controller, the I/O device, or the controlled device at periodic intervals for security-related data;

a validation component that automatically assesses security capabilities of the at least one of the industrial controller, the I/O device, or the controlled device based upon a comparison of the security-related data and one or more predetermined security guidelines; and

a security analysis tool that recommends at least one network interconnection to achieve a specified security goal indicated by the predetermined security guidelines.

20. The system of claim 19, wherein the security guidelines are automatically determined.

21. The system of claim 46, wherein the host-based component performs vulnerability scanning and auditing on devices, and the network-based component performs vulnerability scanning and auditing on networks.

22. (Cancelled)

23. The system of claim 21, wherein at least one of the host-based component or the network-based component at least one of non-destructively maps a topology of information technology (IT) and industrial automation devices, checks revisions and configurations, checks user attributes, or checks access control lists.

24. (Cancelled)

25. The system of claim 17, wherein the security action includes at least one of automatically correcting the security events, automatically adjusting security parameters, altering network traffic patterns, adding security components, removing security components, triggering alarms, automatically notifying entities about detected problems and concerns, generating an error or log file, generating a schema, generating data to re-configure or re-route network connections, updating a database, or updating a remote site.

26-29. (Cancelled)

30. (Currently Amended) An automated security validation system for use in an industrial automation environment having an industrial controller, an I/O device, and a controlled device, the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the industrial controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the industrial controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store a control program that uses the I/O table to control the controlled device, comprising:

means for monitoring communication of data associated with the I/O table with respect to the industrial controller during a training period and establishing a learned pattern of communication;

means for defining a pattern threshold specifying an allowable deviation from the learned pattern;

means for monitoring a current pattern of communication of the data associated with the I/O table subsequent to the training period; and

means for initiating a security procedure that performs a security action to bring the current pattern in line with the learned pattern if the means for monitoring identifies that a current access pattern deviates from the at least learned pattern in excess of the allowable deviation.

31-40. (Cancelled)

41. The tool of claim 1, further comprising a validation component that periodically monitors the controller following deployment of the one or more security outputs to determine one or more vulnerabilities related thereto.

42-44. (Cancelled)

45. The tool of claim 1, the analyzer component is adapted for partitioned security specification entry and sign-off from various groups.

46. The system of claim 19, the scanner component and the validation component are at least one of a host-based component or a network-based component.

47. The system of claim 21, at least one of the host-based component or the network-based component at least one of determines susceptibility to common network-based attacks, searches for open Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports, scans for vulnerable network services, attempts to gain identity information about end devices that relates to hacker entry, or performs vulnerability scanning and auditing on firewalls, routers, security devices, and factory protocols.

48. The system of claim 41, the validation component automatically installs one or more security components in response to the one or more vulnerabilities.

49. The system of claim 1, wherein the analyzer component further performs an automated action that disables network requests from at least one outside network upon detecting that the current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation.

50. The system of claim 12, wherein the at least one automated security event includes at least disabling network attempts to access the industrial controller.

51. The method of claim 12, wherein the monitoring communication of data comprises at least one of monitoring a number of network requests to or from the industrial controller over a given time frame or monitoring a type of request to or from the industrial controller during the training period.

52. The tool of claim 1, wherein the one or more security outputs alter the data traffic between the controller and the at least one I/O device to restore the learned pattern.

IX. Evidence Appendix (37 C.F.R. §41.37(c)(1)(ix))

None.

X. Related Proceedings Appendix (37 C.F.R. §41.37(c)(1)(x))

None.